

MARALYN M. ENGLISH (8468)
JILL L. DUNYON (5948)
SNOW CHRISTENSEN & MARTINEAU
10 Exchange Place, 11th Floor
P.O. Box 45000
Salt Lake City, UT 84145
Telephone: 801-521-9000
Facsimile: 801-363-0400
mme@scmlaw.com
jld@scmlaw.com

DEREK A. NEWMAN (*pro hac vice*)
NEWMAN DU WORS
100 Wilshire Boulevard, Suite 940
Santa Monica, CA 90401
(310) 359-8200
dn@newmanlaw.com

Attorneys for Adknowledge, Inc.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH, CENTRAL DIVISION

XMISSION, L.C., a Utah company,

Plaintiff,

vs.

ADKNOWLEDGE, INC. a Missouri
Corporation; DOES 1-40,

Defendants.

**DEFENDANT ADKNOWLEDGE, INC.'S
MEMORANDUM IN OPPOSITION TO
MOTION FOR TEMPORARY
RESTRAINING ORDER AND REQUEST
FOR PRELIMINARY INJUNCTION**

Case No. 2:15-cv-00277 TC

Judge Tena Campbell

Plaintiff XMission, L.C. did not serve Defendant Adknowledge Inc. with the Complaint or Motion for Temporary Restraining order. Nor did XMission provide notice of this hearing. Adknowledge learned about this case and motion two days before the scheduled status

conference. With almost no time to investigate XMission's claim, Adknowledge files this opposition to the motion for temporary restraining order and preliminary injunction.

I. INTRODUCTION

XMission seeks a TRO based on email that it has not presented to Adknowledge or the Court. Without that evidence, the Court cannot determine whether anybody violated CAN-SPAM. But if anyone violated the law—which is unlikely—Adknowledge is not liable. Adknowledge did not send any email to XMission's customers, and Adknowledge has compliance policies in place to ensure that no company that works with it violates the law. Those policies, and Adknowledge's active policing of businesses that work with it, are enough under the law to immunize Adknowledge even if there was a CAN-SPAM violation.

XMission does not have standing to bring this case because it was not adversely affected by a CAN-SPAM violation. The only harm it complains about is spam issues that Internet service providers typically have. That routine harm does not qualify XMission to “unlock the treasure trove of the CAN-SPAM Act's statutory damages” as one federal circuit court described it.

Nor would XMission suffer irreparable harm if an injunction does not issue. For months on end, XMission collected emails for this case to increase its statutory damages. But it never notified Adknowledge of these allegations, and still hasn't served process even though XMission filed its Complaint weeks ago. By secretly collecting email without asking for it to stop, XMission proved it is not suffering irreparable harm. And since Adknowledge does not send email to XMission, an injunction would not curb the tide of spam to XMission if an injunction issues.

An injunction would not benefit XMission, while it would cause substantial harm to Adknowledge and thousands of legitimate businesses and consumers. The Court should deny XMission's motion for TRO and preliminary injunction.

II. FACTS

A. Adknowledge is a marketing network that did not send any email at issue in this case, and ensures that companies working with it comply with CAN-SPAM and other laws.

1. Adknowledge's business model and compliance policies are set up to prevent the sending of unsolicited commercial email.

2. Adknowledge operates a digital advertising marketplace similar to other large Internet advertisers, including Google and Yahoo. (*See* Decl. of Matt Hoggatt ("Hoggatt Decl."), ¶¶ 2, 19 filed concurrently herewith.)

3. Adknowledge's business units are varied and recognized worldwide as leaders in online marketing, serving over half the Fortune 500 advertisers in the world, including L'Oreal, Range Rover, LG, Samsung, Volkswagen, and Kellogg's. (*Id.* at ¶¶ 5–12.)

4. Online advertising involves three separate actors plus the consumer. The "**publisher**" owns or operates a distribution mechanism leveraging existing relationships with users. (*Id.* at ¶ 14.) The publisher may operate a popular YouTube channel, online merchant sites, social-media sites, popular games or apps, blogs—essentially anybody who can reach the eyes of potential customers. (*Id.*) The "**advertiser**" is a party seeking to generate awareness for and sales of its products and services. (*Id.* at ¶ 15.) The "**marketing network**" has the relationships with publishers and advertisers. (*Id.* at ¶ 16.) The marketing network utilizes sophisticated analytics to match the best customer base with the most relevant advertisers. (*Id.*)

5. Adknowledge is a marketing network. (*Id.*) It connects advertisers with publishers. (*Id.*) The advertiser uses Adknowledge's services to provide links to the advertiser's website. (*Id.*) Adknowledge places those links with publishers. (*Id.* at ¶¶ 16–17.)

6. An advertiser pays Adknowledge each time a customer clicks on a link resulting in a purchase or page view for the advertiser. (*Id.* at ¶ 17.) Adknowledge then pays a commission to the publishers that generated the click. (*Id.*)

7. Adknowledge does not pay publishers—or anyone—for sending commercial emails. (*Id.* at ¶ 18.)

8. Adknowledge does not have a direct relationship with its email publishers’ customers. (*Id.* at ¶ 19.) These publishers must curate their own relationships with their own users. (*Id.*) Adknowledge thus commands no knowledge, rights, or control over the actions of its publishers, including to whom and where those publishers direct email. (*Id.*)

9. Adknowledge requires all email publishers using its technology to represent and warrant that their marketing activities comply with all applicable federal and state laws and regulations, including CAN-SPAM. (*Id.* at ¶ 20.)

10. The emails that XMission complains about may have been sent by publishers working with Adknowledge. But Adknowledge did not send any email at issue in this case. (*Id.* at ¶ 22.) Adknowledge’s “redirect link” as XMission calls it, appears in the emails because Adknowledge tracks consumer clicks for commission purposes—not because Adknowledge caused or induced sending email. (*Id.* at ¶ 23.)

11. Adknowledge only allows publishers to send emails to consenting recipients. (*See* Decl. of John Herbst (“Herbst Decl.”) ¶ 3 filed concurrently herewith.) Adknowledge has a full-time staff of several employees continuously monitoring publishers to ensure they remain compliant with state and federal laws and regulations. (*Id.* at ¶ 4.)

12. Among other requirements, the compliance team ensures that publishers’ email advertisements comply with strict rules regarding headers, content, and unsubscribe links. (*Id.* at ¶ 6.) Adknowledge’s compliance procedures contain detailed steps and policies for virtually every situation encountered in email advertising. (*Id.* at ¶¶ 4, 9–10.) Using sophisticated tools and human review, the compliance team conducts regular audits to ensure compliance, and maintains meticulous record keeping about those audits. (*Id.* at ¶¶ 7, 11–15.) The compliance team runs a weekly dashboard, grading Adknowledge’s compliance success while identifying

and correcting any problems. (*Id.* at ¶ 17.) As the regulatory and business landscape changes, Adknowledge regularly updates its compliance procedures. (*Id.* at ¶ 8.)

13. Adknowledge reacts promptly to consumer requests to be unsubscribed from email marketing, maintaining a “suppression list” that it requires publishers to implement. (*Id.* at ¶ 16.)

14. Publishers found to violate Adknowledge’s rules are notified, fined, and ultimately terminated. (*Id.* at ¶ 19.) Adknowledge’s compliance system specifically hunts down and eliminates “bad actor” publishers that fail to comply with CAN-SPAM. (*Id.*) And Adknowledge uses third-party vendors to identify potential publisher violations. (*Id.*)

15. Due in large part to these compliance procedures, Adknowledge has never been found to violate CAN-SPAM or state laws regulating email marketing. (*Id.* at ¶ 20.)

B. XMission surreptitiously collected emails for months without ever contacting Adknowledge, and alleges Adknowledge is responsible for sending email but did not attach any email for the Court or Adknowledge to review.

16. Plaintiff XMission, L.C. claims to be an Internet service provider that alleges its customers received emails that violate the federal CAN-SPAM Act, but provides no example emails. (*See* XMission, L.C.’s Mot. for TRO and Req. for Prelim. Inj.; Mem. of P. & A. (“TRO”).).

17. XMission cites *Gordon v. Virtumundo* in its TRO motion acknowledging that *every* Internet service provider receives a similar amount of unwanted commercial email. (TRO 6–7.)

18. XMission began collecting the emails for this case in January, but did not file this lawsuit until April. (*Id.* at ¶ 13.) At no time before or during that four-month period did XMission ever contact Adknowledge. (*See* Herbst Decl. ¶ 21.) Even after filing, XMission did not serve process but instead took time to perfect its motion for TRO without any notice to Adknowledge. (*Id.*)

19. XMission alleges its customers received 64,286 commercial emails between January and April 2015 (the “Emails”). (TRO ¶¶13, 18.) XMission claims that Adknowledge’s links

appeared in the Emails. (*Id.* at ¶ 16.) According to XMission, the Emails violate CAN-SPAM because they either (1) originate from IP addresses that do not identify their source, (2) contain generic “from” names, (3) originate from private domains, or (4) originate from domains allegedly designed for email marketing. (*Id.* at ¶¶ 19–20, 22, 24.) A handful of the Emails—364—allegedly include a “from” name that improperly identifies, “a[t] least in part, the intended recipient as the sender of the e-mail.” (*Id.* at ¶ 21.) But because XMission included no example emails, neither the Court nor Adknowledge can verify these allegations.

20. XMission submits no evidence that Adknowledge is responsible for the Emails or owns the domain names from which they were sent. Rather, XMission simply concludes that Adknowledge bears responsibility because Adknowledge’s redirect links appear.

21. XMission offers no evidence that Adknowledge was aware of the Emails, let alone violations of law. XMission simply concludes that the Emails violate CAN-SPAM and further concludes that Adknowledge must not have inquired or confirmed that the emails were sent in compliance with CAN-SPAM.

22. There is no evidence that XMission’s customers did not consent to receiving the Emails.

23. XMission alleges only one remedial measure with respect to the Emails: it used an automated computer process to click on unsubscribe links in each of the Emails. (*Id.* at ¶ 27; *see* Decl. of Peter L. Ashdown (“Ashdown Decl.”) ¶ 40.) XMission claims this effort was unsuccessful. (TRO ¶ 27.) But XMission’s numbers tell a different story. The bulk of the Emails were received in January 2015—43,686—when XMission first started to receive the Emails. (*See* Ashdown Decl. ¶ 94; Ashdown Decl., Ex. 26.) After that, the number of Emails significantly declined. (*Id.*)

24. XMission’s unsubscribe efforts might have been rendered less effective if its customers subscribed again with publishers to receive emails.

C. XMission claims harm from spam over a 20 year period but did not provide any documents or testimony about harm arising from the Emails at issue in this case.

25. XMission claims to have spent considerable money and resources combatting spam. (TRO ¶¶ 28–36.) But XMission does not explain how much of its money or resources were directed to *these* Emails as opposed to spam in general.

26. First, the number of Emails are insignificant. XMission administers approximately 65,000 email accounts on its network. (*Id.* at ¶ 12.) And it complains of the receipt of 64,286 Emails. (*Id.* at ¶ 18.) On average, therefore, XMission customers received *less than one* Email during a single four-month period.

27. Second, XMission indicates enormous expenditure of resources fighting spam. (*Id.* at ¶¶ 28–29.) But XMission is 22 years old. (*Id.* at ¶ 1.) The \$3,000,000 in spam-related expenses cited by XMission occurs over this 22-year period, averaging to about \$135,000 per year. (*Id.* at ¶¶ 28–29.) No specific amounts are described as arising from the Emails and Adknowledge’s actions.

28. XMission worries the Emails will result in loss of customers. (*Id.* at ¶ 45.) But it provides no evidence of such potential loss. And while it claims to have received 6,646 customer complaints related to the Emails, these numbers are suspicious because they appear to rise precipitously while the number of Emails drops dramatically—perhaps in response to XMission’s unsubscribe efforts. (*Id.* at ¶ 39; *see* Ashdown Decl. ¶ 94; Ashdown Decl., Ex. 26.)

D. XMission likely manufactured consumer complaints through an automated computer process, and probably did not receive any real consumer complaints.

29. XMission does not provide any example of a customer complaint. But on January 30, 2015, XMission posted a press release regarding its intent to “take legal action” against spammers and “[a]ll current XMission email customers will participate by default.” (*See* Hoggatt Decl. ¶ 25; *id.*, Ex. A.) Adknowledge suspects—but without discovery, cannot verify—that XMission conducted automatic reporting of “customer complaints” via an automated process. If true, XMission’s “customer complaints” may have involved no action by real people.

30. Adknowledge could only ensure compliance with XMission’s requested TRO by shutting down its entire business. (Hoggat Decl. ¶ 26.)

31. Shutting down Adknowledge’s email business would cost money and cause incalculable long-term harm as advertisers and publishers sought alternatives for their email marketing needs. (*Id.* at ¶ 27.) Adknowledge’s reputation would be damaged and email marketing employees would likely face layoffs. (*Id.*)

III. ARGUMENT

A preliminary injunction is “an extraordinary remedy, and . . . should not be issued unless the movant’s right to relief is ‘clear and unequivocal.’” *Heideman v. South Salt Lake City*, 348 F.3d 1182, 1188 (10th Cir. 2003) (quoting *Kikumura v. Hurley*, 242 F.3d 950, 955 (10th Cir. 2001)). A preliminary injunction (or TRO) requires proof of four factors: (1) substantial likelihood of success on the merits, (2) irreparable harm should the injunction not issue, (3) proof that the threatened injury to the movant outweighs whatever damage the proposed injunction may cause, and (4) proof that the injunction would not be adverse to the public interest. FRCP 65; *Lundgrin v. Claytor*, 619 F.2d 61, 63 (10th Cir. 1980). Of those, the most important is irreparable harm. *Dominion Video Satellite, Inc. v. Echostar Satellite Corp.*, 356 F.3d 1256, 1260 (10th Cir. 2004) (citing *Reuters Ltd. v. United Press Int’l, Inc.*, 903 F.2d 904, 907 (2d Cir. 1990)).

A. XMission is not suffering irreparable harm because the volume of customer complaints is insignificant, and ISPs routinely receive customer complaints.

Courts “consistently not[e] that ‘. . . a showing of probable irreparable harm is the single most important prerequisite for the issuance of a preliminary injunction.’” *Dominion Video Satellite, Inc.*, 356 F.3d at 1260 (quoting *Reuters Ltd.*, 903 F.2d at 907). For that reason, “the moving party must first demonstrate that such injury is likely before the other requirements . . . will be considered.” *Id.* Irreparable harm must be “certain, great, actual ‘and not theoretical.’” *Heideman*, 348 F.3d at 1189 (quoting *Wisconsin Gas Co. v. FERC*, 758 F.2d 669,

674 (D.C. Cir. 1985)). XMission must show “the injury complained of is of such imminence that there is a clear and present need for equitable relief to prevent irreparable harm.” *Heideman*, 348 F.3d at 1189.

1. XMission’s surreptitious email collection for the purpose of increasing its statutory damages, while never providing notice to Adknowledge, shows that XMission is not suffering irreparable harm.

XMission alleges the Emails caused it irreparable harm that will continue without an injunction. If that were true, XMission would have taken action when it first learned about them. Instead, for months on end, XMission surreptitiously collected Emails for the purpose of increasing statutory damages in this case. XMission didn’t file this lawsuit when it first learned of the Emails. It didn’t contact Adknowledge. It didn’t contact any of the email senders.

The vast majority of the Emails supposedly arrived in early January 2015. Even after it filed the Complaint, XMission made no effort to contact Adknowledge. Rather, it let this lawsuit sit idly without service of process while its lawyers perfected a motion for temporary restraining order without notice—presumably for strategic purposes. If XMission legitimately feared irreparable harm, it would have notified Adknowledge prior to filing this lawsuit. XMission’s silence and inaction in the face of “continuous irreparable harm” defies logic and good sense. XMission’s delays do not comport with its allegations of imminent and irreparable harm.

2. An injunction would not prevent harm because the only harm XMission identified is customer complaints and associated loss of competitive position, which will would not change with an injunction against Adknowledge.

XMission identifies its harm as angry customers and declining competitive position. But XMission is in the Internet service provider business, which necessarily involves customer complaints about email. These complaints aren’t harm—they are a necessary and regular part of XMission’s business. Indeed, XMission cites to *Gordon v. Virtumundo*’s acknowledgment admits that *every* internet service provider receives a similar amount of unwanted commercial

email. (TRO 6–7.) If all its competitors face the same degree of unwanted commercial email, the Emails have not caused XMission to lose competitive position.

XMission’s evidence does not identify the percentage of overall complaints that relate to the Emails here, but most likely the Emails here comprise a tiny fraction of overall complaints. Being in the business it is, XMission has always received complaints and always will. An injunction against Adknowledge will not stop complaints, and will not even reduce them. Since Adknowledge did not send the emails, an injunction against Adknowledge will not prevent any emails from reaching XMission. The harm that XMission argues is speculative and unlikely. Because XMission fails to clearly and unequivocally demonstrate “certain, great, and actual” harm, the Court should deny XMission’s motion for a temporary restraining order.

3. XMission’s allegations of harm are limited to its President’s conclusory speculations, unbacked by any supporting evidence or specific detail.

XMission submits no evidence of its harm aside from conclusory statements made by its Chief Technology Officer and President. For example, XMission claims its goodwill and reputation will continue to be harmed by receipt of unwanted commercial email, which could result in loss of customers. (TRO ¶ 13.) But XMission has not alleged that it has lost customers. It does not submit a single customer complaint—most likely because it has never received one relating to these Emails.

XMission does not describe the complaint process, nor does it provide evidence to indicate the complaints relate to the Emails complained about in this case. Instead, it submits raw numbers without any support, which are suspicious. Its numbers indicate declining spam and increasing complaints. For example in January 2015, despite allegedly receiving substantially more spam than in any other month—a total of 43,686—XMission received just 12 customer complaints. (Ashdown Decl., ¶ 94; *id.*, Ex. 26.) The next month saw 4,066 emails generating 63 customer complaints. (*Id.*) Then in March, XMission’s customers received 13,722 emails and

sent 5,301 complaints. (*Id.*) April showed a similar pattern, with 2,803 emails and 1,261 complaints. (*Id.*)

XMission offers no explanation for the sudden and dramatic rise in customer complaints between January and April 2015. Most likely these complaints arose as a result of an automated process that XMission deployed to generate “evidence” for this lawsuit rather than from real customer complaints. *See, supra*, Fact 29. Even assuming the evidence is reliable, XMission provides no evidence that the complained-of increase in commercial email has caused or will cause customer flight.

XMission administers approximately 65,000 email accounts on its network. (TRO ¶ 12). Here it complains of 61,391 alleged spams. (*Id.* at ¶ 13.) So XMission asks this Court to find “irreparable harm” based on an average of *less than one* alleged email per account during a four-month period. Given the public’s familiarity with and ease of eliminating unwanted email (such as deleting the less-than one email per month), XMission has not demonstrated mere “serious or substantial” harm—let alone *irreparable* harm.

Customers who only complain “by default” regarding less than one spam in a four-month period are unlikely to abandon XMission. Without customer statements displaying unhappiness, XMission’s claim that it will lose customers is mere speculation.

The standard for issuing a TRO—“clear and unequivocal” irreparable harm—greatly exceeds that for standing under CAN-SPAM (“significant” harm). *See ASIS Internet Services v. Optin Global, Inc.*, 2008 WL 1902217, at *17 (N.D. Cal. April 28, 2008). Injunctive relief is not appropriate because XMission’s evidence includes (1) no actual example emails alleged to violate the law, (2) nothing but common redirect links connecting Adknowledge to the Emails, and (3) approximately 6,000 customer complaints that XMission apparently generated through its own automated systems.

B. XMission is not likely to succeed on the merits because Adknowledge did not transmit or procure any emails, XMission was not adversely affected to have standing, and XMission has no evidence that any email violated CAN-SPAM.

The CAN-SPAM Act prohibits initiating an email with materially false or misleading header information. 15 U.S.C. § 7704(a)(1) (2012). The term “initiate” means to originate or transmit an email, or to procure email origination or transmission. 15 U.S.C. § 7702(9). The word “procure” means “intentionally to pay or provide other consideration to, or induce, another person to initiate such a message on one’s behalf.” § 7702(12). But when an Internet access provider brings suit with CAN-SPAM, the definition of “procure” expands by adding, “with actual knowledge, or by consciously avoiding knowing, whether such person is engaging, or will engage, in a pattern or practice that violates this chapter.” 15 U.S.C. § 7706(g)(2). This additional scienter element ultimately eliminates XMission’s chances of success on the merits.

Congress’s purpose in enacting CAN-SPAM was not to eradicate commercial email. *Gordon v. Virtumundo*, 575 F.3d 1040, 1049 (9th Cir. 2009). To the contrary, Congress recognized that there are “beneficial aspects to commercial e-mail, even bulk messaging”. *Id.* “Congress wanted to preserve, if not promote” those aspects while targeting “deceptive and predatory practices” and “alleviat[ing] the negative effects of spam without unduly stifling lawful enterprise”. *Id.*

To succeed on the merits, XMission must prove three things: (1) that it has standing, (2) that Adknowledge initiated or procured emails to XMission with scienter, and (3) that those emails contained materially false or misleading headers, or nonworking unsubscribe links. XMission cannot prove any of these.

1. XMission does not have standing because it was not adversely affected by a violation.

Standing under CAN-SPAM requires that an “Internet access service” (“IAS”) suffer particular and substantial “adverse effects.” *Gordon*, 575 F.3d at 1069. XMission understands that *Gordon* clarified the analysis and spills considerable ink defining itself as an “internet access

provider.” But XMission concludes too quickly that it has suffered that “particular type” of real harm as defined by *Gordon*. The harm suffered must be “beyond the mere annoyance of spam and greater than the negligible burdens typically borne by an IAS provider in the ordinary course of business.” *Id.* at 1054. Indeed, *Gordon* specifically cautions courts to “be careful to distinguish the ordinary costs and burdens associated with operating an [IAS] from actual harm.” *Id.* Legitimate service providers are expected to “secure adequate bandwidth and storage capacity and [to] take reasonable precautions, such as implementing spam filters, as part of [] normal operations.” *Id.*

Having IAS status and suffering the right types of harm does not automatically grant standing. *Id.* at 1052–54. The harm must be “attributable” to prohibited practices—the provider must be “*adversely affected by misconduct.*” *Id.* at 1054. (emphasis in original). Therefore, courts should find, “at a bare minimum, a demonstrated relationship between purported harms and...a showing that the identified concerns are linked in some meaningful way to unwanted spam and, in turn, represent actual harm.” *Id.* In this case, XMission cites its general spam-fighting practices but not anything specific to these Emails. XMission claims it spends \$130,000 per year fighting spam, but that seems reasonable for “ordinary costs and burdens associated with operating an [IAS]” as opposed to actual harm. *Id.* Those costs don’t seem more than necessary to “secure adequate bandwidth and storage capacity and [to] take reasonable precautions, such as implementing spam filters, as part of [] normal operations.” *Id.*

XMission attempts to conclude and suppose its right to “unlock the treasure trove of the CAN-SPAM Act’s statutory damages.” *Id.* Drawing heavily from the court’s analysis in *Facebook v. Power Ventures*, XMission compares itself to Facebook in order to show harm. *Facebook v. Power Ventures*, 844 F. Supp. 2d 1025 (N.D. Cal. 2012). But XMission’s analysis puts the cart before the horse. XMission offers *no evidence* that these Emails caused harm, that Adknowledge is responsible for them, or that XMission’s harm can be traced in any way to

Adknowledge's marketing activities on the Internet. Even if XMission correctly argues that 60,000 "spam" emails create *Gordon*-type harm, it still must show that those emails actually violate the law—a burden XMission cannot meet without evidence. XMission has not demonstrated standing, let alone a probability of success on the merits.

2. Adknowledge did not initiate or procure any email at issue in this case.

By reviewing the redirect links that XMission provided, Adknowledge confirmed that it did not originate, transmit, or procure any of the Emails. *See, supra*, Fact 10. XMission makes wild assumptions about Adknowledge's business model without doing any real investigation. Adknowledge provides legitimate advertising for major companies. For example, Geico, the national insurance company, is an advertiser that uses Adknowledge's services to request that customers interested in purchasing auto insurance be directed to its websites. Adknowledge uses its knowledge and analysis of its publisher network to locate publishers with users who may be particularly likely to buy car insurance. *See* Fact 5–6. Adknowledge then mobilizes those publishers, who may send emails to their users. If those users click on links related to car insurance, they get directed to Geico's websites and Adknowledge receives payment. *Id.* Adknowledge then pays a commission to the publisher. *Id.* In order for this to work, Adknowledge must track emails, openings of those emails, and actual user clicks. *Id.* at Fact 10. For those reasons, Adknowledge's "redirect links" appear in the Emails. *Id.*

But Adknowledge only allows publishers to include redirect links in email to already-established consumers. *Id.* Adknowledge's agreements require that publishers only email consumers who have consented to receiving emails from those publishers because Adknowledge itself lacks any control over publisher actions. *Id.* at Facts 8, 11. For example, an electronics retailer who sells car stereos may be well-suited to include links to insurance services when it emails newsletters to its customer base. Such links which would be "redirect links" to Adknowledge's advertiser, Geico. If a consumer clicks on the link, Geico receives traffic and

pays Adknowledge, which in turn pays a commission to the electronics-retailer publisher for the click.

If the publisher does not place the redirect link in its email, it still nonetheless sends the email. Adknowledge never pays or induces publishers or anyone else to send emails. Adknowledge pays for clicks, and prohibits publishers from sending email with redirect links to anybody who didn't request email from the publisher. Adknowledge did not directly send any emails with the redirect links that XMission provides, nor did it pay anyone else to send them.

XMission also alleges that Adknowledge knew or consciously avoided knowing that its publishers send spam emails. (TRO at 8–10.) XMission dredges up a couple small lawsuits to prove that Adknowledge was “on notice” of its illegal activities. *Id.* But in both *Zoobuh* (where Adknowledge was the plaintiff) and *Carper* (which was not a CAN-SPAM case), Adknowledge was successful. Adknowledge has never lost a CAN-SPAM or state-law email case on the merits.

XMission fails to offer evidence of Adknowledge's knowledge—or conscious avoidance of knowledge—that any of its publishers relevant to this case engaged in patterns or practices that violated CAN-SPAM. Instead, XMission assumes not only that the Emails violate CAN-SPAM, but that they are so “full of patent and readily identifiable” violations that Adknowledge must have “failed to take the proper steps to inquire and confirm” that its publishers abide by the law. (TRO at 10.)

But Adknowledge's compliance and monitoring policies and procedures create robust consumer protections designed to *ensure* that—not ignore whether—its publishers and affiliates follow the law. *See supra*, Facts 10–16. When violations are identified—which would be accomplished faster if complainants like XMission swiftly notified Adknowledge of specific concerns—Adknowledge takes action to fine or terminate the responsible publisher. *Id.* at Fact 16. XMission could never show that Adknowledge acted “with actual knowledge, or by consciously avoiding knowing, whether such person is engaging, or will engage, in a pattern or

practice that violates” CAN-SPAM. Adknowledge lacks the scienter required for liability, even if someone violated the law.

For these reasons, XMission cannot succeed on the element that Adknowledge initiated or procured an email, and therefore cannot demonstrate a likelihood of success on the merits.

3. No email in this case contained a materially false or misleading header, or nonworking unsubscribe link.

XMission must prove that the Emails contain, or are accompanied by, header information that is materially false or materially misleading. For that reason, the most important evidence in this case is the Emails. But XMission provides no evidence of the Emails, even for illustrative purposes. Instead, XMission submits a self-serving declaration from its president describing emails that it never attaches.

Hearsay is an out-of-court statement used to prove the truth of the matter asserted in the statement. Fed R. Evid. 801(c). Unless an exception applies, hearsay is inadmissible. Fed R. Evid. 802. Similarly, the best-evidence rule requires that an original document be submitted to prove its content—unless an exception applies, a summary is inadmissible. Fed. R. Evid. 1002. The Emails are an out-of-court statement of allegedly false or deceptive headers. XMission attempts to prove the Emails have false or misleading headers—not by attaching them—but by describing them. By not attaching the emails, XMission violated the hearsay and best-evidence rules. Thus, there is no evidence of any email in this case.

Adknowledge concedes that some publishers send its redirect links by email. But each of the publishers must agree to Adknowledge’s policies. *See, supra*, Facts 8–9. Those policies are lengthy and include requirements that publishers never send false or misleading email, and describe the various type of email prohibited. *Id.* at Fact 8. Adknowledge carefully polices its publishers through a full-time compliance team comprised of several employees. *Id.* at Facts 11–13. Publishers failing to comply with Adknowledge’s requirements may not continue the privilege of advertising for Adknowledge’s marketing network. *Id.* at Fact 16. For that reason,

even if a publisher sent an email to XMission, almost certainly that email would not contain a false or misleading header.

XMission also suggests the Emails violate CAN-SPAM for lacking operable unsubscribe mechanisms. (TRO at 15.) XMission believes the unsubscribe links were not operable because some of its customers received emails after XMission attempted to opt consumers out using an automated process. *Id.* at Fact 29. But since Adknowledge publishers only send to consumers with which they have relationships, any customer who XMission unsubscribed may have signed up again. *Id.* There is no reason to believe that XMission's customers did not re-subscribe or take other steps to ensure receipt after XMission's unsubscribe efforts. Nor is there any evidence from any actual consumer that it received an email from a publisher after clicking on an unsubscribe link.

XMission cannot succeed on the merits of its claim because (1) it lacks standing since it was not adversely affected by a violation, (2) Adknowledge did not initiate or procure any email, and (3) XMission lacks evidence of any email that has false or misleading headers or a nonworking unsubscribe link.

C. The balance of equities tips strongly in Adknowledge's favor because XMission cannot prevent most its spam with the injunction it requests, whereas Adknowledge would have to shut down an entire business effecting tens of thousands of customers

Adknowledge cannot comply with XMission's requested injunction because it does not send the email that XMission complains about. If an injunction issues, Adknowledge can prohibit its publishers from including redirect links in emails to XMission, but that will not stop email from flowing to XMission. *See, supra*, Fact 7. The publisher can continue to send email, just with other links.

The injunction that XMission requests is too broad. The relief requested would put Adknowledge at risk for contempt if XMission received any email with an Adknowledge redirect link. The only way Adknowledge could comply is by shutting down its business entirely. *See,*

supra, Fact 33. Shutting down the business for any period of time will cause long-term injury to Adknowledge's business. *Id.* at Fact 34. Advertisers and publishers will take their business elsewhere. *Id.* Adknowledge's reputation and ability to conduct other areas of business will suffer incalculable harm. *Id.* Jobs will be lost. *Id.*

In contrast, withholding an injunction would simply mean business as usual for XMission: collecting emails for this litigation, which it was willing to do for months without complaint. XMission will still receive spam, and the volume of that spam will not decrease.

D. The public interest weighs against an injunction because email recipients have an interest in receiving messages they requested, advertisers have an interest in lawfully promoting legitimate products, and publishers have an interest in providing a forum for advertisers.

An injunction will also adversely affect businesses who rely on Adknowledge to promote their products and provide information to consumers who have requested email from companies they have a relationship with. *See, supra*, Fact 3. An injunction will adversely affect consumers who have requested commercial email and will not receive it, and publishers who have a right to promote products to their customers.

CAN-SPAM notes a substantial government interest in commercial email regulation. But it also recognizes the legitimacy and importance of commercial email and bulk messaging. 15 U.S.C. § 7701(b) (recognizing importance of national rules for commercial email); § 7704 (creating requirements for transmission of commercial email thereby presupposing legitimacy); *Gordon*, 575 F.3d at 1049 (noting the “beneficial aspects” to commercial email and Congress’s intention to preserve even bulk messaging as a “worthwhile commercial tool.”).

XMission offers no evidence that its customers do not want the Emails. In fact, XMission admits it assumed what its customers wanted and attempted to unsubscribe on their behalf “by default.” (TRO Facts 26–27.) There is no way of knowing whether XMission’s customers solicited the Emails and would oppose an injunction or not.

E. The Court should not issue an injunction because it lacks personal jurisdiction over Adknowledge.

The Court also lacks personal jurisdiction over Adknowledge. Adknowledge is a resident of Delaware and Missouri. And the Due Process Clause only permits personal jurisdiction over nonresident defendants that have certain minimum contacts with the forum state. *See Shrader v. Biddinger*, 633 F.3d 1235, 1239 (10th Cir. 2011).

The minimum contacts standard is met by showing the defendant “has purposefully directed [its] activities at residents of the forum, and the litigation results from alleged injuries that arise out of or relate to those activities.” *Intercon, Inc. v. Bell A. Internet Solutions, Inc.*, 205 F.3d 1244, 1247 (10th Cir. 2000). In the internet context, this means an “internet user or site intentionally directed his/her/its activity or operation at the forum state rather than just having the activity or operation accessible there.” *Shrader*, 633 F.3d at 1240.

In *Fenn v. Mleads Enterprises, Inc.*, 2006 UT 8, ¶ 26, the Utah Supreme Court found that unsolicited email to a Utah resident did not give rise to personal jurisdiction. That case did not involve the volume of email alleged in this case, but the analysis still applies. Like in *Fenn*, there is no “substantial connection to Utah.” Adknowledge did not target Utah and could never have anticipated being sued here. For that reason, Adknowledge is not subject to jurisdiction gave rise to jurisdiction.

Here, there is no evidence Adknowledge purposefully directed any commercial emails to residents of Utah because there is no evidence that Adknowledge directs commercial emails to *anyone*. There is no evidence Adknowledge conducted substantial or continuous local activity in Utah. The exercise of personal jurisdiction in such a case would be unreasonable and would violate the notions of fair play and substantial justice.

F. Given that an injunction will force Adknowledge to shut down its business, XMission should be required to post a substantial bond if the injunction issues.

XMission fails to prove any of the requirements necessary for issuing an injunction. If the Court disagrees, it should require XMission to “give[] security in an amount that the court

considers proper to pay the costs and damages sustained” by Adknowledge. FRCP 65(c). XMission requests an injunction without the required security without citing to legal support. (See TRO § VI.) Instead, XMission argues that because customers may opt out of receiving the Emails, and XMission has unsuccessfully attempted to unsubscribe, that an injunction “preserves the parties’ rights” and creates a “status quo.” *Id.*

XMission presents no evidence that the Emails are unsolicited, or that the Emails lack a functional unsubscribe link. *See supra*, § III.B. If this TRO issues, Adknowledge must effectively shut down its email marketing business, costing it tens of millions of dollars in lost revenue and possibly endangering the company’s health. *See, supra*, § III.C. For these reasons, Adknowledge respectfully requests the Court require XMission to provide security in an amount to be determined before issuing any injunction. That amount should be at least \$100 million, which Adknowledge would prove through evidence filed under seal.

IV. CONCLUSION

XMission did not file this lawsuit because it suffered harm. If it suffered harm, XMission would have notified Adknowledge of these allegations months ago and at least served it with the complaint and motion for TRO. Instead, XMission sandbags Adknowledge with a TRO status conference without any notice, and virtually no time to respond or investigate. This lawsuit is not about redress—this is a money grab by a company believing spam litigation is a new lucrative business model.

There is no evidence of the Emails, let alone that Adknowledge initiated or procured them. There is no evidence of irreparable harm—in fact, XMission sat on its rights for months. An injunction would force Adknowledge to shutter its business. If that were not enough, it appears the Court lacks personal jurisdiction over Adknowledge.

Adknowledge respectfully requests the Court deny XMission’s motion for temporary restraining order and/or preliminary injunction.

DATED this 4th day of May, 2015.

SNOW, CHRISTENSEN & MARTINEAU

/s/ Maralyn M. English

Maralyn M. English

Jill L. Dunyon

Derek A. Newman (*pro hac vice*)

NEWMAN DU WORS

100 Wilshire Boulevard, Suite 940

Santa Monica, CA 90401

(310) 359-8200

Attorneys for Adknowledge, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on the 4th day of May, 2015, I electronically filed the foregoing **DEFENDANT ADKNOWLEDGE, INC.'S MEMORANDUM IN OPPOSITION TO MOTION FOR TEMPORARY RESTRAINING ORDER AND REQUEST FOR PRELIMINARY INJUNCTION** with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the CM/ECF participants registered to receive service.

*/s/ Maralyn M. English*_____

3224060